

Notice of Allowability

Application No.

09/927,671

Examiner

Tamara Teslovich

Applicant(s)

FINK ET AL.

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to Amendments filed August 22, 2005.
2. ☒ The allowed claim(s) is/are 1-52.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
 5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

This action is in response to the Amendments filed on August 22, 2005.

Claims 1-2, 6-7, 10-11, 16-17, 21-22, 25-26, 30-31, 35-36, 39-40, 44-45, and 48-49 have been amended.

Claims 1-52 are herein considered.

Response to Arguments

Applicant's arguments filed August 22, 2005 have been fully considered and treated as follows:

Claims 1-52 are allowed.

Applicant's newly amended claims 1-52 comprise allowable subject matter of allowable claims, finding clear support in the specifications and containing no new matter.

Examiner's Amendment

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Joseph R. Palmieri on December 8, 2005.

Application/Control Number: 09/927,671
Art Unit: 2137

Page 3

The application has been amended as follows:

Please amend Claims in accordance with Examiner's "Amendment to Claims"
included as pages 4-15 of this office action.

AMENDMENT TO CLAIMS

Please replace existing claims 1-52 with claims 1-52 below.

1. A network security apparatus for securing packet header information of a data packet, comprising:
 - a key exchanger adapted to derive a cipher key;
 - a translator adapted to translate predetermined portions of said packet header information according to a cipher algorithm keyed by the cipher key into translated packet header information, and replace said predetermined portions of said packet header information with the translated packet header information in the data packet; and
 - a communication device adapted to communicate the data packet between a first enclave and a second enclave through a wide area network;wherein said predetermined portions of said packet header information include a destination host address portion that identifies a destination host within the second enclave, a destination port number and a sequence parameter that changes on a per-packet basis.
2. A network security apparatus as set forth in Claim 1, wherein the predetermined portions of packet header information further comprise:
 - a source host address portion that identifies a sending host within the first enclave.
3. A network security apparatus as set forth in Claim 1, wherein said translator is adapted to queue the data packet until said key exchanger has derived the cipher key.
4. A network security apparatus as set forth in Claim 1, wherein said key exchanger further comprises:

a timer adapted to reset at a predetermined time interval, wherein said key exchanger derives the cipher key when said timer resets and the data packet is present at said translator.

5. A network security apparatus as set forth in Claim 1, wherein the wide area network is the Internet.

6. A network security apparatus for securing packet header information of a data packet, comprising:

a random number generator adapted to generate a random number;

a translator adapted to translate predetermined portions of said packet header information according to a cipher algorithm seeded by the random number into translated packet header information, and replace said predetermined portions of said packet header information with the translated packet header information in the data packet; and

a communication device adapted to communicate the data packet between a first enclave and a second enclave through a wide area network;

wherein said predetermined portions of said packet header information include a destination host address portion that identifies a destination host within the second enclave, a destination port number and a sequence parameter that changes on a per-packet basis.

7. A network security apparatus as set forth in Claim 6, wherein the predetermined portions of packet header information further comprise:

a source host address portion that identifies a sending host.

8. A network security apparatus as set forth in Claim 6, further comprising:

a timer adapted to reset at a predetermined time interval, wherein said random number generator derives the random number when said timer resets and the data packet is received by said translator.

9. A network security apparatus as set forth in Claim 6, wherein the wide area network is the Internet.

10. A network security system for securing packet header information of a data packet communicated between a first enclave and a second enclave through a wide area network, the system comprising:

- a first communication device in communication with the first enclave and the wide area network, said first communication device adapted to receive the data packet, translate predetermined portions of said packet header information into translated packet header information and replace said predetermined portions of said packet header information with the translated packet header information in the data packet, and place the data packet on the wide area network; and

- a second communication device in communication with the second enclave and the wide area network, said second communication device adapted to receive and restore the predetermined portions of the data packet from the translated packet header information and place the data packet onto the second enclave;

- wherein said predetermined portions of said packet header information include a destination host address portion that identifies a destination host within the second enclave, a destination port number and a sequence parameter that changes on a per-packet basis.

11. A network security system as set forth in Claim 10, wherein the predetermined portions of packet header information further comprise:

- a source host address portion that identifies a sending host within the first enclave.

12. A network security system as set forth in Claim 10, further comprising:

- a key exchanger coupled to said first and second communication devices, adapted to derive a cipher key; and

a timer electrically coupled to said key exchanger, adapted to reset at a predetermined time interval.

13. A network security system as set forth in Claim 12,
wherein said key exchanger derives the cipher key when said timer resets and the first communication device receives the data packet, and

wherein said first and second communication devices translate the predetermined portions of packet header information according to a cipher algorithm keyed by the cipher key.

14. A network security system as set forth in Claim 12, wherein said first and second communication devices are adapted to queue the data packet until the key exchanger has derived the cipher key.

15. A network security system as set forth in Claim 10, wherein the wide area network is the Internet.

16. A method for securing packet header information of a data packet, comprising:

deriving a cipher key;

translating predetermined portions of said packet header information according to a cipher algorithm keyed by the cipher key into translated packet header information;

replacing said predetermined portions of said packet header information with the translated packet header information in the data packet; and

communicating the data packet between a first enclave and a second enclave through a wide area network;

wherein said predetermined portions of said packet header information include a destination host address portion that identifies a destination host within the second enclave, a destination port number and a sequence parameter that changes on a per-packet basis.

17. A method for securing packet header information as set forth in Claim 16, wherein the predetermined portions of packet header information further comprise:

a source host address portion that identifies a sending host within the first enclave.

18. A method for securing packet header information as set forth in Claim 16 further comprising:

queuing the data packet until the cipher key has been derived.

19. A method for securing packet header information as set forth in Claim 16 further comprising:

deriving the cipher key at a predetermined time interval if the data packet to be communicated has been presented to said translating step.

20. A method for securing packet header information as set forth in Claim 16 wherein the wide area network is the Internet.

21. A method for securing packet header information of a data packet, comprising:

generating a random number;

translating predetermined portions of said packet header information according to a cipher algorithm seeded by the random number into translated packet header information;

replacing said predetermined portions of said packet header information with the translated packet header information in the data packet; and

communicating the data packet between a first enclave and a second enclave through a wide area network;

wherein said predetermined portions of said packet header information include a destination host address portion that identifies a destination host within the second enclave, a destination port number and a sequence parameter that changes on a per-packet basis.

22. A method for securing packet header information as set forth in Claim 21, wherein the predetermined portions of packet header further comprises:

a source host address portion that identifies a sending host.

23. A method for securing packet header information as set forth in Claim 21, further comprising:

deriving the random number at predetermined time interval if the data packet to be communicated has been presented to said translating step.

24. A method for securing packet header information as set forth in Claim 21, wherein the wide area network is the Internet.

25. A method for securing packet header information of a data packet, comprising:

receiving the data packet at a first communication device;

translating predetermined portions of packet header information into translated packet header information;

replacing said predetermined portions of said packet header information with the translated packet header information in the data packet;

sending the data packet to a second enclave through a wide area network;

receiving the data packet at a second communication device on the second enclave;

restoring translating the predetermined portions of the data packet from the translated packet header information at the second communication device; and

placing the data packet onto the second enclave;

wherein said predetermined portions of said packet header information include a destination host address portion that identifies a destination host within the second enclave, a destination port number and a sequence parameter that changes on a per-packet basis.

26. A method for securing packet header information as set forth in Claim 25, wherein the predetermined portions of packet header information further comprise:

- a source host address portion that identifies a sending host within the first enclave.

27. A method for securing packet header information as set forth in Claim 25, further comprising:

- deriving a cipher key at a predetermined time interval if the data packet is presented to the first communication device; and

- translating the predetermined portions of packet header information for the data packet according to a cipher algorithm seeded by the cipher key.

28. A method for securing packet header information as set forth in Claim 27, further comprising:

- queuing the data packet until the cipher key has been derived.

29. A method for securing packet header information as set forth in Claim 25, wherein the wide area network is the Internet.

30. A communication device adapted for processing packet header information of a data packet, the communication device being operable to:

- derive a cipher key;

- translate predetermined portions of said packet header information according to a cipher algorithm keyed by the cipher key into translated packet header information;

- replace said predetermined portions of said packet header information with the translated packet header information in the data packet; and

- communicate the data packet between a first enclave and a second enclave through a wide area network;

- wherein said predetermined portions of said packet header information include a destination host address portion that identifies a destination host within the second

enclave, a destination port number and a sequence parameter that changes on a per-packet basis.

31. A communication device as set forth in Claim 30, wherein the predetermined portions of packet header information further comprise:

 a source host address portion that identifies a sending host within the first enclave.

32. A communication device as set forth in Claim 30, the communication device being further operable to queue the data packet until the cipher key has been derived.

33. A communication device as set forth in Claim 30, the communication device being further operable to derive the cipher key at a predetermined time interval if the data packet to be communicated has been generated.

34. A communication device as set forth in Claim 30, wherein the wide area network is the Internet.

35. A communication device adapted for processing packet header information of a data packet, the communication device being operable to:

 generate a random number;

 translate predetermined portions of said packet header information according to a cipher algorithm seeded by the random number into translated packet header information;

 replace said predetermined portions of said packet header information with the translated packet header information in the data packet; and

 communicate the data packet between a first enclave and a second enclave through a wide area network;

 wherein said predetermined portions of said packet header information include a destination host address portion that identifies a destination host within the second

enclave, a destination port number and a sequence parameter that changes on a per-packet basis.

36. A communication device as set forth in Claim 35, wherein the predetermined portions of packet header further comprises:

a source host address portion that identifies a sending host.

37. A communication device as set forth in Claim 35, the communication device further operable to derive the random number at predetermined time interval if the data packet to be communicated has been presented to the communication device.

38. A communication device as set forth in Claim 35, wherein the wide area network is the Internet.

39. A device for securing packet header information of a data packet, comprising:

means for deriving a cipher key;

means for translating predetermined portions of said packet header information according to a cipher algorithm keyed by the cipher key into translated packet header information;

means for replacing said predetermined portions of said packet header information with the translated packet header information in the data packet; and

means for communicating the data packet between a first enclave and a second enclave through a wide area network;

wherein said predetermined portions of said packet header information include a destination host address portion that identifies a destination host within the second enclave, a destination port number and a sequence parameter that changes on a per-packet basis.

40. A device for securing packet header information as set forth in Claim 39, wherein the predetermined portions of packet header information further comprise:

a source host address portion that identifies a sending host within the first enclave.

41. A device for securing packet header information as set forth in Claim 39, further comprising:

means for queuing the data packet until the cipher key has been derived.

42. A device for securing packet header information as set forth in Claim 39, further comprising:

means for deriving the cipher key at a predetermined time interval if the data packet to be communicated has been presented to said means for translating.

43. A device for securing packet header information as set forth in Claim 39, wherein the wide area network is the Internet.

44. A device for securing packet header information of a data packet, comprising:

means for generating a random number;

means for translating predetermined portions of said packet header information according to a cipher algorithm seeded by the random number into translated packet header information;

means for replacing said predetermined portions of said packet header information with the translated packet header information in the data packet; and

means for communicating the data packet between a first enclave and a second enclave through a wide area network;

wherein said predetermined portions of said packet header information include a destination host address portion that identifies a destination host within the second enclave, a destination port number and a sequence parameter that changes on a per-packet basis.

45. A device for securing packet header information as set forth in Claim 44, wherein the predetermined portions of packet header further comprises:

a source host address portion that identifies a sending host.

46. A device for securing packet header information as set forth in Claim 44, further comprising:

means for deriving the random number at predetermined time interval if the data packet to be communicated has been presented to the means for translating.

47. A device for securing packet header information as set forth in Claim 44, wherein the wide area network is the Internet.

48. A device for securing packet header information of a data packet, comprising:

means for receiving the data packet at a first communication device;

means for translating predetermined portions of packet header information into translated packet header information;

means for replacing said predetermined portions of said packet header information with the translated packet header information in the data packet;

means for sending the data packet to a second enclave through a wide area network;

means for receiving the data packet at a second communication device on the second enclave;

means for translating the predetermined portions of the data packet at the second communication device; and

means for placing the data packet onto the second enclave;

wherein said predetermined portions of said packet header information include a destination host address portion that identifies a destination host within the second enclave, a destination port number and a sequence parameter that changes on a per-packet basis.

49. A device for securing packet header information as set forth in Claim 48, wherein the predetermined portions of packet header information further comprise:

a source host address portion that identifies a sending host within the first enclave.

50. (Original) A device for securing packet header information as set forth in Claim 48, further comprising:

means for deriving a cipher key at a predetermined time interval if the data packet to be communicated has been presented to the first communication device; and

means for translating the predetermined portions of packet header information for the data packet according to a cipher algorithm seeded by the cipher key.

51. A device for securing packet header information as set forth in Claim 50, further comprising:

means for queuing the data packet until the cipher key has been derived.

52. A device for securing packet header information as set forth in Claim 48, wherein the wide area network is the Internet.

Allowable Subject Matter

The following is an examiner's statement of reasons for allowance:

The present invention is directed to an apparatus and method for providing adaptive self-synchronized dynamic address translation in order to conceal the identities of LAN machines and local network topologies from adversaries. Each independent claim identifies the uniquely distinct features of replacing the destination host address portion, destination port number, and sequence parameter with the translated destination host address portion, translated destination port number, and designated sequence parameter respectively, according to the cipher algorithm keyed by the cipher key. The closest prior art, Caronni (US Patent No. 6,507,908 B1), discloses a method and apparatus for network address translation involving translating network addresses to secure IP addresses before passing the packets onto the network. Nowhere does Caronni teach translating only the host portion of the destination address and the destination port number and sequence parameter and replacing the initial header portions with their translated portions. Friedman et al. (US Patent No. 5,757,924) also provides device and process for translating network addresses securely, however Friedman employs an encipher function to encrypt the message content, translating the entire address as a whole before sending the packet out onto the network. The remaining references cited by the Examiner rely upon methods which either replace the entire header with a translated packet enclosing the old packet as an encrypted content,

Art Unit: 2137

or replace addresses within the header according to session keys decided upon by the sending and receiving machines. The prior art, either singularly or in combination fails to anticipate or render obvious the present invention and its limitations of replacing the network portion of header destination addresses, destination ports and sequence numbers with portions individually encrypted with a key cipher.

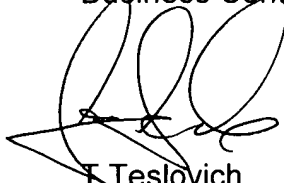
Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571) 272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



T. Teslovich
December 7, 2005



MATTHEW SMITHERS
PRIMARY EXAMINER